



## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets <sup>6</sup> : <b>H04L 29/06</b>	<b>A1</b>	(11) Numéro de publication internationale: <b>WO 97/33415</b> (43) Date de publication internationale: 12 septembre 1997 (12.09.97)
--	-----------	--

(21) Numéro de la demande internationale: PCT/FR97/00371

(22) Date de dépôt international: 3 mars 1997 (03.03.97)

(30) Données relatives à la priorité:  
96/02901 7 mars 1996 (07.03.96) FR(71) Déposant (pour tous les Etats désignés sauf US): CP8  
TRANSAC [FR/FR]; 68, route de Versailles, F-78430  
Louvenciennes (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (US seulement): SIGAUD, Alain [FR/FR];  
12, hameau de la Vallée, F-78990 Elancourt (FR).(74) Mandataire: CORLU, Bernard; Bull S.A., 68, route de  
Versailles, F-78434 Louvenciennes (FR).(81) Etats désignés: AU, BR, CA, CN, JP, KR, NO, SG, US, brevet  
européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE,  
IT, LU, MC, NL, PT, SE).

Publiée

Avec rapport de recherche internationale.

(54) Title: METHOD ENABLING SECURE ACCESS BY A STATION TO AT LEAST ONE SERVER, AND DEVICE USING SAME

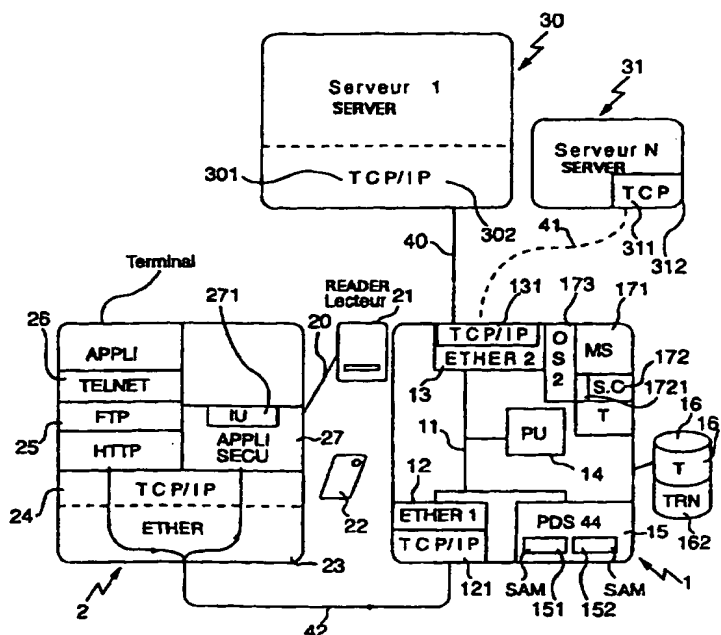
(54) Titre: PROCÉDE DE SECURISATION DES ACCES D'UNE STATION A AU MOINS UN SERVEUR ET DISPOSITIF METTANT  
EN OEUVRE LE PROCÉDE

## (57) Abstract

A server access securing method and a device using same are disclosed. The method for securing access to at least one server (30) enables secure access by user stations (2) to at least one application server via a network (42) that uses a multisession, multipoint telecommunication protocol. The method comprises the steps of systematically establishing a parallel security session between the user station (2) and a security processor (1) connected between the user station to be protected during application sessions and the server(s) (30) to be protected, and cyclically initiating a security session.

## (57) Abrégé

La présente invention concerne un procédé de sécurisation des accès à des serveurs et le dispositif mettant en oeuvre le procédé. Le procédé de sécurisation des accès à au moins un serveur (30) est caractérisé en ce qu'il permet de sécuriser les accès en provenance de stations (2) d'utilisateur et à destination d'au moins un serveur d'application à travers un réseau (42) utilisant un protocole de télécommunication multi sessions et multi ports, ledit procédé consiste en une étape d'établissement systématique d'une session de sécurité en parallèle entre la station d'utilisateur (2) et un processeur de sécurité (1) interposé entre la station d'utilisateur à protéger pendant le déroulement des sessions d'applications et le ou les serveurs (30) à protéger et une étape de déclenchement cyclique de session de sécurité.





(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平10-506744

(43) 公表日 平成10年(1998) 6月30日

(51) IntCl. <sup>6</sup>	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 A
13/00	3 5 7	13/00 3 5 7 Z
H 0 4 L 29/08		H 0 4 L 13/00 3 0 7 Z

審査請求 有 予備審査請求 未請求(全 20 頁)

(21) 出願番号 特願平9-531514  
(86) (22) 出願日 平成9年(1997) 3月3日  
(85) 翻訳文提出日 平成9年(1997) 11月7日  
(86) 国際出願番号 PCT/FR 97/00371  
(87) 国際公開番号 WO 97/33415  
(87) 国際公開日 平成9年(1997) 9月12日  
(31) 優先権主張番号 96/02901  
(32) 優先日 1996年3月7日  
(33) 優先権主張国 フランス (FR)  
(81) 指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, L U, MC, NL, PT, SE), AU, BR, CA, C N, J P, KR, NO, SG, US

(71) 出願人 ブル・セー・ペー・8  
フランス国、エフ・78430・ループシエンヌ、ペー・ペー・45、ルート・ドウ・ベルサイユ、68  
(72) 発明者 シゴー、アラン  
フランス国、エフ・78990・エランクール、アモー・ドウ・ラ・バレ、12  
(74) 代理人 弁理士 川口 義雄 (外2名)

(54) 【発明の名称】 ステーションから少なくとも一つのサーバへの接続を安全化する方法、およびこの方法を使用する装置

(57) 【要約】

本発明は、ステーションから少なくとも一つのサーバへのアクセスを安全化する方法、およびこの方法を使用する装置に関する。少なくとも一つのサーバ (30) へのアクセスを安全化する方法は、ユーザステーション (2) から出され、マルチセッションおよびマルチポート通信プロトコルを使用するネットワーク (42) を通して少なくとも一つのアプリケーションサーバに向けたアクセスを安全化することができ、ユーザステーション (2) と、アプリケーションのセッションの進行中保護すべきユーザステーションと保護すべき単数または複数のサーバ (30) の間に間置されるセキュリティプロセッサ (1) との並行セキュリティセッションを系統的に確立する段階と、セキュリティセッションを周期的に起動する段階とを含むことを特徴とする。

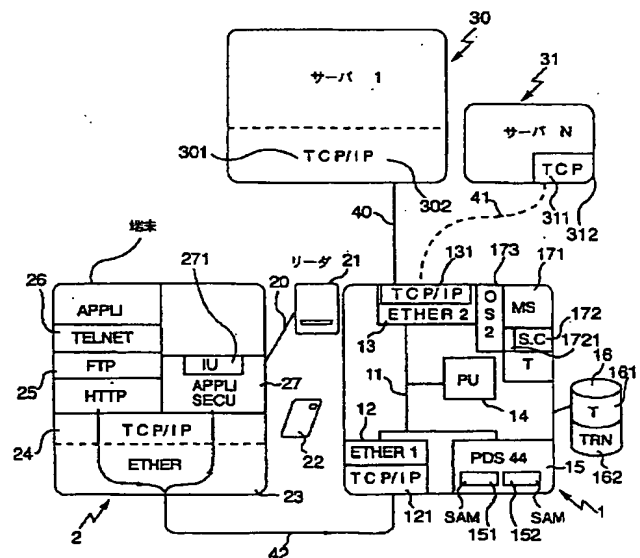


Fig.1

**【特許請求の範囲】**

1. 少なくとも一つのサーバ(30)へのアクセスを安全化する方法であって、ユーザステーション(2)から出され、マルチセッションおよびマルチポート通信プロトコルを使用するネットワーク(42)を通して少なくとも一つのアプリケーションサーバに向けたアクセスを安全化することができ、

— ユーザステーション(2)と、アプリケーションのセッションの進行中保護すべきユーザステーションと保護すべき単数または複数のサーバ(30)との間に間置されるセキュリティプロセッサ(1)との並行セキュリティセッションを系統的に確立する段階と、

— セキュリティセッションを周期的に起動する段階とを含むことを特徴とする方法。

2. セキュリティセッションを系統的に確立する段階が、

送信元IPアドレスおよび、ステーション(2)が要求するアプリケーションに組み合わせられる少なくとも一つのポート番号を、ステーションからネットワークに送信する段階と、

アプリケーションに組み合わせられる安全手順をセキュリティ

プロセッサが検索する段階と、

セキュリティプロセッサ(1)とステーション(2)との間にセキュリティセッションを確立する段階と、

アプリケーション用に使用されるリモートサーバの名称およびアドレスを、セキュリティプロセッサ(1)がローカルファイルで検索し、IPアドレスおよびポート番号を通信することにより、リモートサーバ(30、31)との接続を開始する段階と

を含むことを特徴とする請求の範囲第1項に記載の少なくとも一つのサーバへのアクセスを安全化する方法。

3. アプリケーションに組み合わせられる手順が、ステーション(2)と、セキュリティプロセッサが選択するリモートサーバ(30)との間に接続を直接確立することから成ることを特徴とする請求の範囲第2項に記載の少なくとも一つのサ

サーバへのアクセスを安全化する方法。

4. 実施すべきであって、記憶された表内で規定された安全手順により、ユーザの認証、ユーザの確認、ユーザ権の管理、確認、暗号化キーの計算、署名の計算、サーバ上で要求されるアプリケーションへの選択的アクセスを与えるためのユーザのプ

ロフィルの確認などの機能のうちの単数または複数を選択できることを特徴とする請求の範囲第1項に記載の少なくとも一つのサーバへのアクセスを安全化する方法。

5. セキュリティプロセッサが、接続の連番、接続開始および終了年月日および時刻、送信元IPアドレスおよび少なくとも一つのポート番号、使用セキュリティオブジェクトの識別子、選択リモートサーバの名称、送信先IPアドレス、ポート番号、実行規約を含むログ(162)をメモリ(16)内に記憶することを特徴とする請求の範囲第1項に記載の少なくとも一つのサーバへのアクセスを安全化する方法。

6. セキュリティプロセッサ(1)が、プロセッサによって処理されるアプリケーションのリスト、接続の種類に応じて行うべき処理、実施すべき安全手順、ブラックリスト、ホワイトリスト、および加入者リストの定義によるユーザのアクセス権、リモートサーバへのアクセス許可スケジュールを、メモリ(16)の第二表(161)内に記憶することを特徴とする請求の範囲第1項に記載の少なくとも一つのサーバへのアクセスを安全化する方法。

7. ユーザステーション(2)から出され、マルチセッション

およびマルチポート通信プロトコルを使用するネットワーク(42)を通して少なくとも一つのアプリケーションサーバに向けたアクセスをセキュリティプロセッサ(1)を使用して安全化し、ポータブルメディア、およびステーション(2)に組み合わされたポータブルメディアリーダー(21)とのやり取り、ならびにマルチセッションおよびマルチポート通信プロトコル(24)とのやり取りを管理するために、ステーション上にセキュリティソフトウェア(27)が置かれて

いる装置であって、セキュリティプロセッサ(1)が、ステーション(2)と、ステーション(2)が要求するアプリケーションに応じてセキュリティプロセッサが選択したサーバ(30)との間に通信を確立する手段(12、13)と、その通信を管理する手段(14、15、172、171)とを含むことを特徴とする装置。

8. 通信を確立し管理する手段により、ステーション(2)とサーバとの間で直接通信を確立するか、動作に必要なメモリを具備するマイクロプロセッサを含み、通信サーバ(172)およびセキュリティエンジン(171)のプログラムを実行する主プロセッサ(14)によって決定される安全手順を解釈することができる安全管理モジュールMCSと通信する安全装置に

よって管理されるセキュリティセッションの確立後、ステーション(2)とサーバとの間で通信を確立することができることを特徴とする請求の範囲第7項に記載の装置。

9. 通信を確立する手段(12、13)が二つの通信カードから成り、一方がステーションに接続され、他方が、サーバ接続され、マルチセッションおよびマルチポート通信プロトコルによりステーションおよびサーバと通信することを特徴とする請求の範囲第7項に記載の装置。

**【発明の詳細な説明】****ステーションから少なくとも一つのサーバへの接続を  
安全化する方法、およびこの方法を使用する装置**

本発明は、ステーションから少なくとも一つのサーバへの接続を安全化する方法、およびこの方法を使用する装置に関する。

サーバおよびステーション間通信網内で、とくに、サーバの支援を得てステーションにおいて実行されるアプリケーションのために通信が重要な情報を使用する時に、通信の安全化がはかられていることは周知である。従来の安全化の原則は、アプリケーションとネットワークの通信プロトコルの層との間に、安全化プログラムの一部を付加することであった。このプログラム層は端末上およびサーバ上に設置されていた。このような方法の欠点は、同方法が、アプリケーションまたは通信層の変更、および本来の意味での安全化プログラムと特定のアプリケーションとの間のインタフェースを実現するプログラミングの一部分を必要とすることである。したがって各アプリケーションについて、特定のプログラムインタフェースを開発する必要がある。また、端末がマルチサーバネットワークに接続されている限り、各サーバを安全化しなければならない。各アプリケ

ーションに必要なプログラミング時間は、各サーバを安全化する必要性和相俟って、アプリケーションを安全化するのに必要な予算を大きく圧迫するようになっていた。

本発明の目的は、端末上で実行されるアプリケーションプログラムの変更およびサーバの変更を一切必要としない安全化方法を提供することである。

この目的は、この方法により、ユーザステーションから出され、マルチセッションおよびマルチポート通信プロトコルを使用するネットワークを通して少なくとも一つのアプリケーションサーバに向けたアクセスを安全化することができることによって達成される。

この方法は、

— ユーザステーションと、アプリケーションのセッションの進行中保護すべきユーザステーションと保護すべき単数または複数のサーバの間に間置されるセ

セキュリティプロセッサとの並行セキュリティセッションを系統的に確立する段階と、

ー セキュリティセッションを周期的に起動する段階と  
を含む少なくとも一つのサーバへのアクセスを安全化する方法によって達成される。

別の特徴によれば、セキュリティセッションを系統的に確立する段階は、

送信元IPアドレスおよび、ステーションが要求するアプリケーションに組み合わされる少なくとも一つのポート番号を、ステーションからネットワークに送信する段階と、

アプリケーションに組み合わされる安全手順をセキュリティプロセッサが検索する段階と、

セキュリティプロセッサとステーションとの間にセキュリティセッションを確立する段階と、

アプリケーション用に使用されるリモートサーバの名称およびアドレスを、セキュリティプロセッサがローカルファイル内で検索し、IPアドレスおよびポート番号を通信することにより、リモートサーバとの接続を開始する段階とを含む。

別の特徴によれば、アプリケーションに関連する手順は、ステーションと、セキュリティプロセッサが選択するリモートサーバとの間に接続を直接確立することから成る。

別の特徴によれば、実施すべきであって、記憶された表内で規定された安全手順により、ユーザの認証、ユーザの確認、ユ

ーザ権の管理、確認、暗号化キーの計算、署名の計算、サーバ上で要求されるアプリケーションへの選択的アクセスを与えるためのユーザのプロファイルの確認などの機能のうちの単数または複数を選択できる。

別の特徴によれば、セキュリティプロセッサは、接続の連番、接続開始および終了年月日および時刻、送信元IPアドレスおよび少なくとも一つのポート番号



、使用セキュリティオブジェクトの識別子、選択リモートサーバの名称、送信先IPアドレス、ポート番号、実行規約を含むログを大容量メモリに記憶する。

別の特徴によれば、セキュリティプロセッサは、プロセッサによって処理されるアプリケーションのリスト、接続の種類に応じて行うべき処理、実施すべき安全手順、ブラックリスト、ホワイトリスト、および加入者リストの定義によるユーザのアクセス権、リモートサーバへのアクセス許可スケジュールを、メモリの第二表に記憶する。

本発明の別の目的は、この方法を利用することができる装置を提供することである。

この目的は、本装置により、カード、および端末に組み合わ

されたカードリーダーとのやり取り、ならびにマルチセッションおよびマルチポート通信プロトコルとのやり取りを管理するセキュリティソフトウェアが置かれる端末と、セキュリティプロセッサが、ステーションと、ステーションが要求するアプリケーションに応じてセキュリティプロセッサが選択したサーバとの間に通信を確立する手段と、その通信を管理する手段とを含むことを特徴とするセキュリティプロセッサとの間でこの方法を使用することができることによって達成される。

別の特徴によれば、通信を確立し管理する手段により、端末とサーバとの間で直接通信を確立するか、動作に必要なメモリを具備するマイクロプロセッサを含み、通信サーバおよびセキュリティエンジンのプログラムを実行する主プロセッサによって決定される安全手順を解釈することができる安全管理モジュールMCSと通信する安全装置によって管理されるセキュリティセッションの確立後、端末とサーバとの間で通信を確立することができる。

別の特徴によれば、通信を確立する手段が、たとえばイーサネット、トークンリングなど二つのローカルエリアネットワークカードから成り、一方がステーションに接続され、他方が、

サーバに接続され、マルチセッションおよびマルチポート通信プロトコルにより

ステーションおよびサーバと通信する。

本発明の他の特徴および長所は、添付の図面を参照して行う以下の説明を読むことにより、より明らかになるう。

第 1 図は、安全化方法を使用することができる装置の原理の略図である。

第 2 A 図は、端末の安全化ソフトウェアによって管理されるダイアログボックスを示す図である。

第 2 B 図は、リーダまたはカードがないことを知らせる別のダイアログボックスを示す図である。

第 2 C 図は、搬送コードを要求する別のダイアログボックスを示す図である。

第 2 D 図は、相手先のサーバの選択ができる別のダイアログボックスを示す図である。

第 2 E 図は、文字列の入力ができる別のダイアログボックスを示す図である。

第 2 F 図は、主ウィンドウを示す図である。

次に第 1 図および第 2 図を参照しながら、本発明について説明する。本発明は、結合路 (42、40、41) から成るネッ

トワークを通して、単数または複数のサーバ (30、31) との間で通信する端末 (2) から成るネットワーク上に設置される。端末は、サーバのネットワークに局所的に接続するか、接続ネットワーク、GSM、RNI S などあらゆる種類の通信ネットワークを通して接続する可動携帯型マイクロコンピュータとすることができる。このようなネットワーク上では、たとえば TELNET 型の遠隔地端末サービスアプリケーション、たとえば FTP などのファイル転送サービス、HTTP などのインターネットによって使われるプロトコル、あるいは現在知られている他のあらゆるアプリケーションが走る。ネットワークは、たとえば TCP/IP プロトコルなどのマルチセッションおよびマルチポート型の通信プロトコル 24 で動作する端末のコンピュータ上のイーサネット (23) 型のローカルエリアネットワークカードから成る。各サーバ (30、31) もイーサネットカード (302、312)、および組み合わされる TCP/IP プロトコル (301、311) を含む。ネットワークが複数のサーバを含む場合、ネットワークを

安全化するためには、サーバと同じエンクロージャ内にあるサーバのジャンクションノードに、ネットワークの単数または複数の端末(2)と

対話するセキュリティプロセッサ(1)を間置するだけでよい。各端末(2)は、ソフトウェア(27)から成るセキュリティアプリケーションと、ポータブルメディア(22)のリーダー(21)との物理的結合路(20)とを具備する。これらポータブルメディア(22)は、チップカードまたはPC/MCIA型カードとすることができる。

セキュリティプロセッサ(1)は、PC(パーソナルコンピュータ)型電子カードと対応するメモリとを含む処理装置(14)から成り、バス(11)により、それぞれ結合路(40、41)によって各サーバ(30、31)に接続されるイーサネット型第一ネットワークカード(13)、および結合路(42)により端末に接続されるイーサネット型第二ネットワークカード(12)と通信を行う。バス(11)は、処理装置と、図示しないメモリと、安全チェックモジュールMCS(S. A. M Security Application Module)(151、152)とを含む安全化アプリケーションカード(15)とも通信を行う。設備は、それぞれがn個の安全チェックモジュールMCS(151、152)を含むn個のカードを含むことができる。リーダー(21)およびポータブルメディアをとまなうこれらの

モジュールMCS(151、152)により、基本秘密キーの不可侵性を確保しつつ、認証、証明、暗号化キーの計算などのセキュリティ機能を実行することができる。これらのセキュリティ機能は、チップカード、またはリーダー(21)により端末(2)のセキュリティアプリケーション(27)に接続されたらポータブルメディア(22)に含まれる情報も活用する。処理装置(14)は、セキュリティプロセッサ(1)が複数のタスクを並行して実行できるように、たとえばOS2型のマルチタスクオペレーティングシステム(173)上で動作する。各イーサネットカード(12、13)は、TCP/IPプロトコル(131、121)などネットワークに固有の通信プロトコルを使用することができるソフトウ

エア階層を含む。処理装置（14）は、オペレーティングシステムに加え、TCP/IP型ネットワークのプロトコルにより第一カード（13）と第二カード（12）との間の通信の処理をすることができる階層（1721）を含む通信サーバ（172）とともに動作する。この通信サーバ（172）は、第二イーサネットカード（12）と、サーバに接続された第一カード（13）との間の結合を直接行うべきか、あるいは安全手順を実施した後にしかこの結合

を行うことができないかどうかを判定する役割を有する。この判定は、メモリ（16）内に記憶され、アプリケーションと実施すべき少なくとも一つの安全手順との間の対応表を含むファイルAPPLI.INIを読むことにより、行われる。実施の場合、この通信サーバはセキュリティエンジン（171）を利用し、セキュリティエンジンは、セキュリティ機能を実行することができるセキュリティプロセッサ（1）の安全化アプリケーションカード（15）の動作を起動する。セキュリティエンジンMSにより、セキュリティネットワークを構成すること、セキュリティプロセッサによって処理されるアプリケーションのリストを作成すること、実行された処理を規定すること、実施すべき安全手順を規定すること、ユーザのアクセス権および許可スケジュールを規定することができる。端末内に置かれたセキュリティアプリケーション（27）も、ソフトウェアWindows（登録商標）などのウィンドウ表示型オペレーティングシステム上で走る。ステーションで一旦セキュリティソフトウェア（27）のロードが行われると、セキュリティソフトウェアにより端末のユーザは、セキュリティアプリケーションの起動後に主ウィンドウ（第2図）が表示されることによ

って、セキュリティ接続を起動すること、セキュリティ接続を切ること、あるいはアプリケーションから抜けることができる。第2F図に示すように、使用可能な三つの機能のうちのいずれかを選択するには、所期の機能のところにハイライト部分をもっていき、マウスの「クリック」またはキーボードの「enter」キーを押す。ユーザは、セキュリティプロセッサ（1）のIPアドレス、および使用を希望するアプリケーションに割り当てられたポート番号（たとえばセキ

リティアプリケーションの場合X、FTPアプリケーションの場合21、Telnetの場合23など）を指定することにより、安全化ネットワークに接続する。セキュリティプロセッサ（1）は対応表内で、ステーションから送られるポート番号に組み合わされている安全手順を検索し、とくにユーザポータブルメディア（22）の認証およびカード所有者コード（P. I. N.）によるユーザの確認をとまなう安全手順を実施するためにセキュリティアプリケーション（27）との通信を確立する。

任意には、セキュリティプロセッサ（1）は、アプリケーションのリスト、ホワイトリストとして定義されたユーザが利用許可されたもの、およびブラックリストとして定義されたユー

ザが許可されていないものをステーション上に表示させることができる。次にユーザは、キーボードまたはマウスを操作することにより、サーバ・アプリケーション対の選択を行う。ユーザは、安全手順が正常に実行されたら、選択肢を確定することにより、選択したアプリケーション（Telnet、FTP、HTTP、...）を起動する。セキュリティプロセッサ（1）は端末（2）からアプリケーションに対応するポート番号を受け取り、対応表内で、アプリケーションサーバのIPアドレスを決定し、要求されたアプリケーションサーバへの通信を確立する。端末（2）とサーバ（30、31）のうちのいずれかとの間で接続が確立されると、セキュリティプロセッサは端末（2）への周期的セキュリティチェックを行うことにより、確立されたアプリケーションセッションを監視する。セキュリティ異常検出時（カードの取り出し、無動作、署名の計算不良など）には、セキュリティプロセッサ（1）はリモートサーバへの接続を中断し、セキュリティセッションを中止する。

複数の安全手順を実行することができ、起動している手順の選択は、接続データ内に示されるアプリケーションのポート番号に応じて行われる。これらポート番号および結合されている

手順についての情報は、セキュリティプロセッサ（1）の大容量メモリ（16）

の表(161)の一部を構成するファイルACCUEIL. CAM内にある。セキュリティ接続を起動する際には、データの表示および入力、送信元および送信先IPアドレスの管理、パスワードによるアクセスの管理、所持者の確認、安全モジュールMCS、数値化、署名、証明の計算、情報の読み出しおよび書き込み、カードの取り出しの確認を基にした認証、表T(161)の一部を構成するアクセス権およびリストである、ブラックリスト、ホワイトリスト、加入者リスト内での、リモートサーバへのユーザのアクセス権の確認を可能とするスマートカードによるアクセスの管理、通信プロトコルTCP/IPの種々のサービスの使用権の確認、ユーザ、または選択したマシンのアクセスに関し許可され、列方向に時間範囲、行方向にユーザまたはマシンのIDを含む表となる、時間および日付の範囲の確認、などの処理のうちの任意の単数または複数の処理を行うことができる受け入れ手順を使用する。カスタマイドメニューの表示により、ユーザに関して許可されているアプリケーションまたはリモートサーバのうちの一つを選択することができる。ファイルAPPLI. INIにより、

実行すべき安全手順ならびに実行時間をメモリ(16)内に記憶し、アプリケーションに応じて識別することができ、これにより、手順および選択した実行時間に応じて、選択したリモートサーバのアプリケーションに従って、手順の実行を周期的に開始することができる。周期手順は、端末のカードに、手順によって選択された情報(乱数)の電子署名を行うよう要求することにより、リモートユーザが権利を有するユーザであることを確認する。手順はMCSを使用して、これらの署名が、適切な秘密キーを有するカードによって生成されたものであることを確認する役割を有する。この方法により、とくに、ネットワーク上の侵入装置によるIPアドレスの盗難を未然に防ぐことができる。ユーザがリモートサーバおよびアプリケーションを選択すると、セキュリティプロセッサは、アプリケーションのポート番号を回収し、ローカルファイルを使用して、セキュリティプロセッサが選択したリモートサーバとの接続を開始する。セキュリティプロセッサが選択したこのリモートサーバは、ユーザが示すサーバと異なってもよい。ユーザは、セキュリティプロセッサを通して通信を受け取るだけである。これら

の通信は、ステーション（２）のポート番号により、ステーショ

ンに送られる。最後に、セキュリティプロセッサはセキュリティエンジン（１７１）により、接続の連番、接続開始および終了年月日および時刻、送信元ＩＰアドレスおよびポート番号、使用セキュリティオブジェクトの識別子、選択リモートサーバの名称、送信先ＩＰアドレス、ポート番号、アプリケーションセッション時、ステーションとサーバとの間でやり取りされるデータの量、実行規約を記憶する接続ログ（１６２）を大容量メモリ（１６）内に保存することができる。セキュリティアプリケーション（２７）は、第一ダイアログボックス（第２Ａ図）を表示することにより、ユーザにパスワードの入力と、次に、このワードの確定、またはセキュリティ接続の切断を行う、操作のキャンセルとを要求することができるように、オペレーティングシステムWindowsのウィンドウおよびダイアログボックス形式表示システムを使用することができるプレゼンテーションモジュール（２７１）を含む。また、ユーザインタフェースによっても、「リーダにカードなし」（carte absente d'lecteur）および「カードを挿入して下さい」（veuillez inserervotre carte SVP）のメッセージを表示する第二ダイアログボックス（第２Ｂ図）、ならびに手順の確定またはキャンセルボ

タンによりカード所持者のコードを入力することができる第三ダイアログボックス（第２Ｃ図）を表示することができる。最後に、第四ダイアログボックスにより、ネットワークの可能なサーバの展開リストの中から選択することにより、送信先サーバの選択をすることができる。他の二つのダイアログボックスについては、その一つにより、セキュリティプロセッサから受信したメッセージを表示することができる、もう一方のダイアログボックス（第２Ｅ図）により、文字列の入力を要求することができる。このようにしてアクセスを安全化し、安全担当者の意思により、アクセス手順の条件を選択することができたことが理解され、さらにセキュリティ接続の周期性により、不正利用者が、ネットワークに接続されている端末の代理となる振りをして、ある時に接続することを防ぐことができる。なぜなら、不正利用者は、端末へのアクセスキーをもっていないからであり、安

全手順は不正利用者を確認することをせず、セッションを禁止する。最後にこの方法は、接続部上を循環するアプリケーションの Protokol とくらべ、透明性を維持している長所を有する。事実、セキュリティシステムのインストレーションは、端末上のアプリケーション、より少なくはサーバ上のアプリケ

ーションを変更することなく行われる。

セキュリティソフトウェア (27) およびセキュリティプロセッサ (1) のインストール時、インストール担当者は、初期化ファイル (SERVEUR. INI) 内で、所与の時間来、アプリケーション接続がない場合、クライアントポストとの間で確立していたセキュリティ接続をプロセッサ (1) が閉じることができるセキュリティ時間、および所与の時間来、アプリケーション接続上でやり取りされるデータがない場合、クライアントポストとの間で確立していたセキュリティ接続およびアプリケーション接続をプロセッサ (1) が閉じることができる非活動時間とを規定する。

また、当業者にとって可能な他の変更も本発明の主旨の一部となる。



【図1】

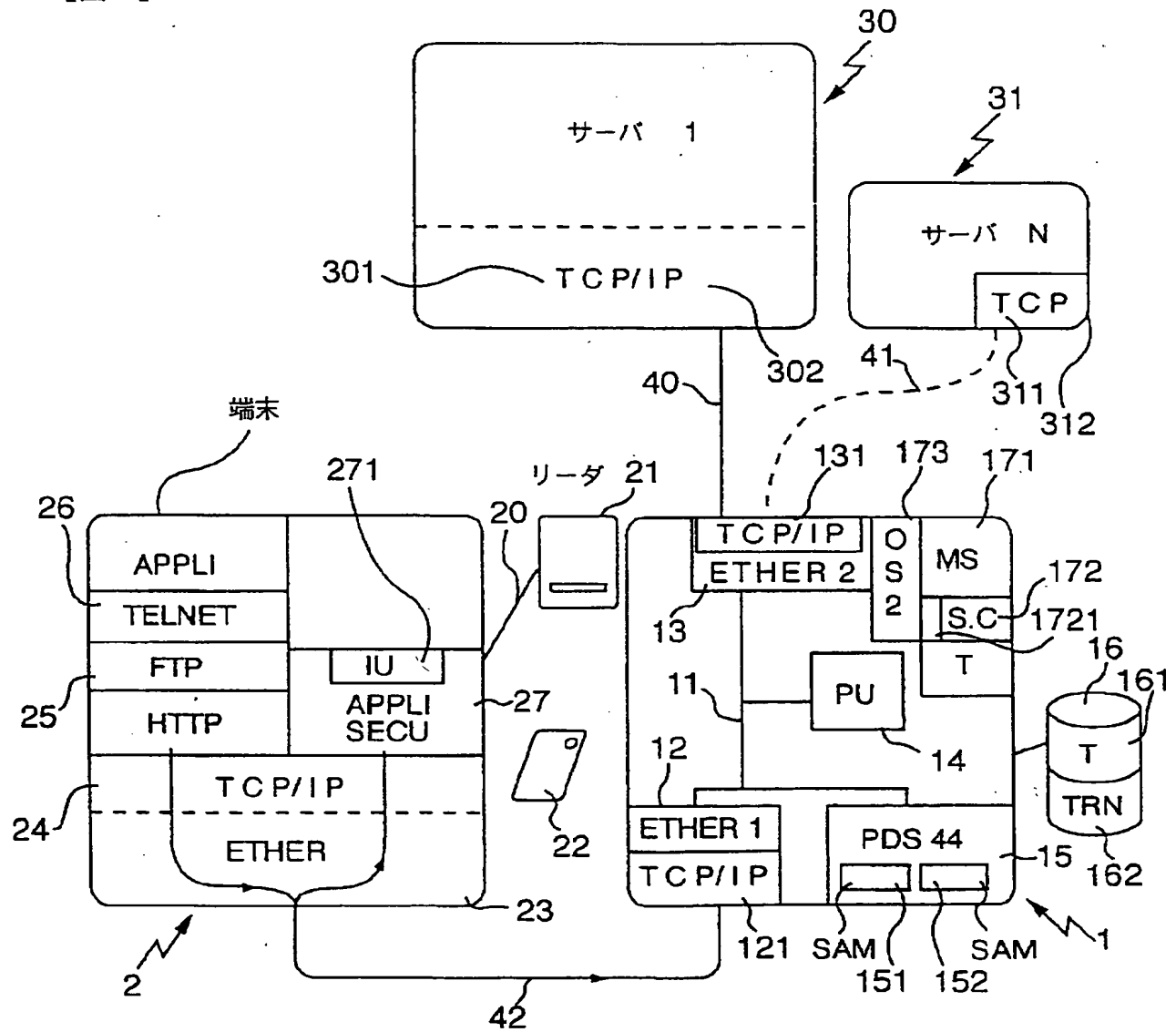
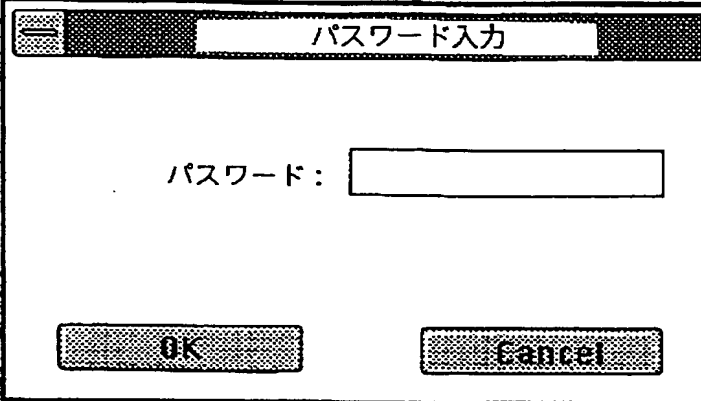


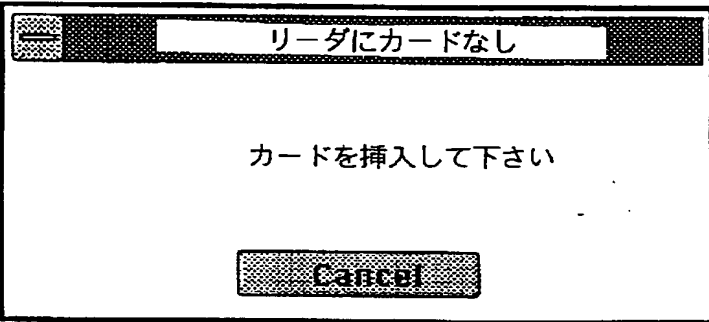
Fig.1

【図2】



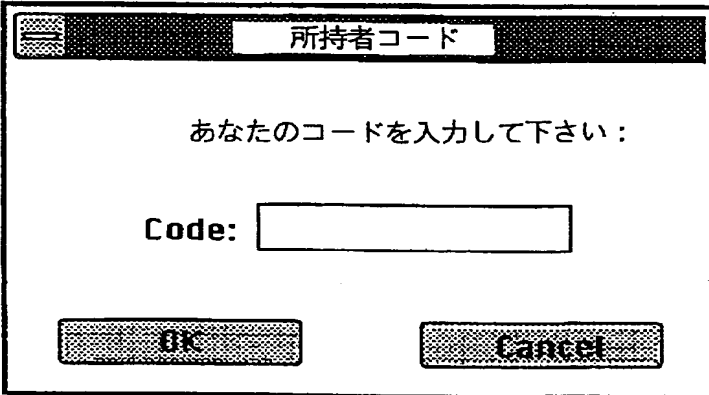
A screenshot of a password input screen. The title bar at the top contains a menu icon and the text "パスワード入力". The main area displays the text "パスワード:" followed by a rectangular input field. At the bottom, there are two buttons: "OK" on the left and "Cancel" on the right.

Fig.2A



A screenshot of a card reader error screen. The title bar at the top contains a menu icon and the text "リーダにカードなし". The main area displays the text "カードを挿入して下さい". At the bottom, there is a single "Cancel" button.

Fig.2B



A screenshot of an owner code input screen. The title bar at the top contains a menu icon and the text "所持者コード". The main area displays the text "あなたのコードを入力して下さい:". Below this text is the label "Code:" followed by a rectangular input field. At the bottom, there are two buttons: "OK" on the left and "Cancel" on the right.

Fig.2C

【図2】

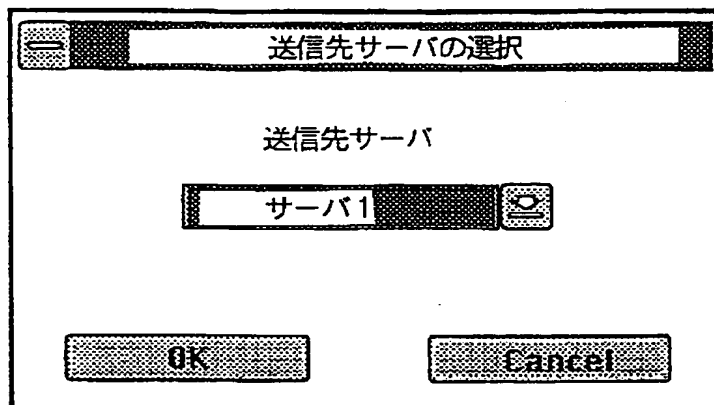


Fig.2D

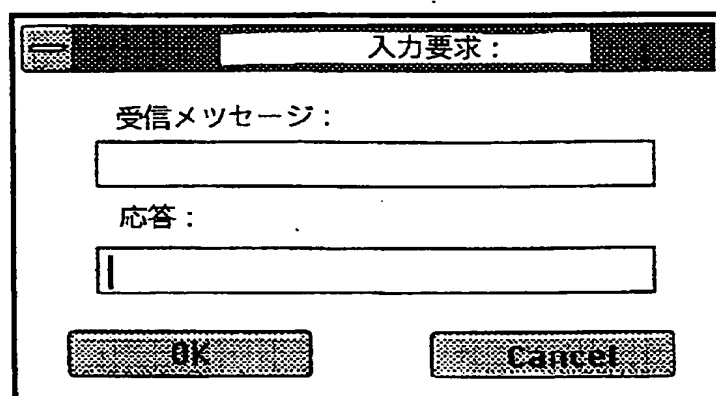
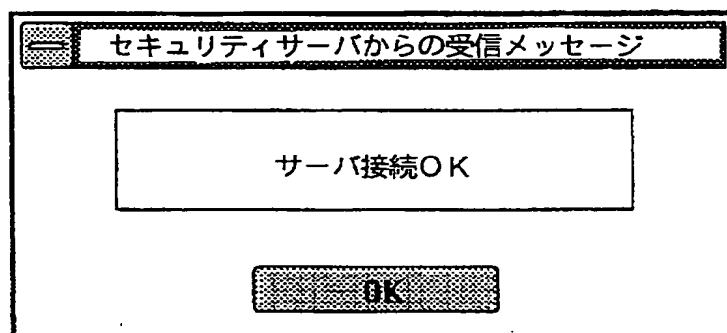


Fig.2E

【図2】

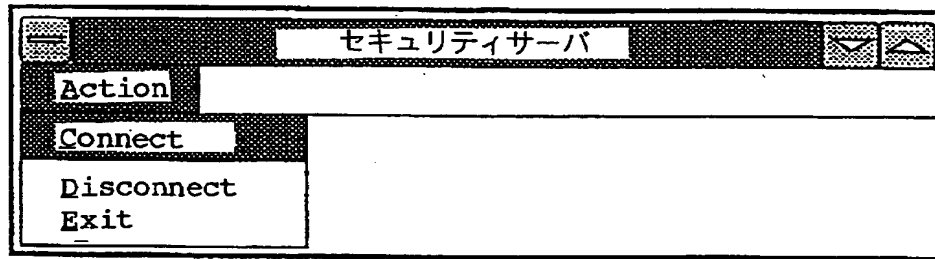


Fig.2F

## 【国際調査報告】

## INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 H04L29/06		International Application No PCT/FR 97/00371
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DATA COMMUNICATIONS, vol. 24, no. 16, 21 November 1995, pages 71-78, 80, XP000545336 NEWMAN D ET AL: "CAN FIREWALLS TAKE THE HEAT?" see page 74, left-hand column - page 77, right-hand column	1-9
A	IEEE COMMUNICATIONS MAGAZINE, vol. 32, no. 9, 1 September 1994, pages 50-57, XP000476555 BELLOVIN S M ET AL: "NETWORK FIREWALLS" see page 51, left-hand column - page 56, left-hand column	1-6
--- -/--		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		
<input type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents:		
"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family		
Date of the actual completion of the international search 9 May 1997		Date of mailing of the international search report 16.05.97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer Goossens, A

## INTERNATIONAL SEARCH REPORT

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		International Application No. PLI/FR 97/00371
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CONNEXIONS, vol. 9, no. 7, 1 July 1995, pages 20-23. XP000564023 TED DOTY: "A FIREWALL OVERVIEW" see the whole document -----	1-6